

What Is Claimed Is:

1 1. A method for facilitating the delegation of operations involved in
2 providing digital signatures to a signature server, the method comprising:
3 receiving a request for a digital signature from a user at the signature
4 server, the request including an item to be signed on behalf of the user by the
5 signature server;
6 looking up a private key for the user at the signature server;
7 signing the item with the private key for the user; and
8 returning the signed item to the user so that the user can send the signed
9 item to a recipient.

1 2. The method of claim 1, wherein prior to signing the item, the
2 method further comprises authenticating the user.

1 3. The method of claim 2, wherein prior to signing the item, the
2 method further comprises determining whether the user is authorized to sign the
3 item.

1 4. The method of claim 3, wherein determining whether the user is
2 authorized to sign the item involves looking up an authorization for the user based
3 upon an identifier for the user as well as an identifier for an application to which
4 the user will send the signed item.

1 5. The method of claim 3, wherein determining whether the user is
2 authorized to sign the item involves communicating with an authority server that
3 is separate from the signature server.

1 6. The method of claim 1, further comprising allowing the user to
2 authenticate the signature server prior to sending the request to the signature
3 server.

1 7. The method of claim 1, further comprising facilitating encryption
2 of communications between the user and the signature server.

1 8. The method of claim 1, wherein the method further comprises
2 configuring the signature server to accommodate a new user by:
3 receiving a request from an authorized entity to add the new user;
4 generating a key pair for the new user, including a new user private key
5 and a new user public key;
6 communicating with a certification authority to obtain a certificate for the
7 new user based on the key pair; and
8 storing the certificate and the key pair for the new user in a location that is
9 accessible by the signature server to enable the signature server to sign items on
10 behalf of the new user.

1 9. The method of claim 1, wherein the method further comprises
2 configuring the signature server to delete an old user by:
3 receiving a request from an authorized entity to delete the old user;
4 notifying a certification authority to revoke a certificate for the old user;
5 and
6 removing the private key for the old user from the signature server, so that
7 the signature server can no longer sign items on behalf of the old user.

1 10. The method of claim 1, wherein the method further comprises
2 archiving the request and the signed item at the signature server.

1 11. The method of claim 1, wherein the method further comprises
2 forwarding the signed item to an archive server in order to be archived.

1 12. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for
3 facilitating the delegation of operations involved in providing digital signatures to
4 a signature server, the method comprising:
5 receiving a request for a digital signature from a user at the signature
6 server, the request including an item to be signed on behalf of the user by the
7 signature server;
8 looking up a private key for the user at the signature server;
9 signing the item with the private key for the user; and
10 returning the signed item to the user so that the user can send the signed
11 item to a recipient.

1 13. The computer-readable storage medium of claim 12, wherein prior
2 to signing the item, the method further comprises authenticating the user.

1 14. The computer-readable storage medium of claim 13, wherein prior
2 to signing the item, the method further comprises determining whether the user is
3 authorized to sign the item.

1 15. The computer-readable storage medium of claim 14, wherein
2 determining whether the user is authorized to sign the item involves looking up an

3 authorization for the user based upon an identifier for the user as well as an
4 identifier for an application to which the user will send the signed item.

1 16. The computer-readable storage medium of claim 14, wherein
2 determining whether the user is authorized to sign the item involves
3 communicating with an authority server that is separate from the signature server.

1 17. The computer-readable storage medium of claim 12, wherein the
2 method further comprises allowing the user to authenticate the signature server
3 prior to sending the request to the signature server.

1 18. The computer-readable storage medium of claim 12, wherein the
2 method further comprises facilitating encryption of communications between the
3 user and the signature server.

1 19. The computer-readable storage medium of claim 12, wherein the
2 method further comprises configuring the signature server to accommodate a new
3 user by:
4 receiving a request from an authorized entity to add the new user;
5 generating a key pair for the new user, including a new user private key
6 and a new user public key;
7 communicating with a certification authority to obtain a certificate for the
8 new user based on the key pair; and
9 storing the certificate and the key pair for the new user in a location that is
10 accessible by the signature server to enable the signature server to sign items on
11 behalf of the new user.

1 20. The computer-readable storage medium of claim 12, wherein the
2 method further comprises configuring the signature server to delete an old user by:
3 receiving a request from an authorized entity to delete the old user;
4 notifying a certification authority to revoke a certificate for the old user;
5 and
6 removing the private key for the old user from the signature server, so that
7 the signature server can no longer sign items on behalf of the old user.

1 21. The computer-readable storage medium of claim 12, wherein the
2 method further comprises archiving the request and the signed item at the
3 signature server.

1 22. The computer-readable storage medium of claim 12, wherein the
2 method further comprises forwarding the signed item to an archive server in order
3 to be archived.

1 23. An apparatus that facilitates delegating operations involved in
2 providing digital signatures, comprising:
3 a signature server;
4 a receiving mechanism within the signature server that is configured to
5 receive a request for a digital signature from a user, the request including an item
6 to be signed on behalf of the user by the signature server;
7 a lookup mechanism within the signature server that is configured to look
8 up a private key for the user;
9 a signing mechanism within the signature server that is configured to sign
10 the item with the private key for the user; and

11 a sending mechanism within the signature server that is configured to
12 return the signed item to the user so that the user can send the signed item to a
13 recipient.

1 24. The apparatus of claim 23, further comprising an authentication
2 mechanism that is configured to authenticate the user prior to signing the item.

1 25. The apparatus of claim 24, further comprising an authorization
2 mechanism that is configured to determine whether the user is authorized to sign
3 the item prior to signing the item.

1 26. The apparatus of claim 25, wherein the authorization mechanism is
2 configured to determine whether the user is authorized to sign the item by looking
3 up an authorization for the user based upon an identifier for the user as well as an
4 identifier for an application to which the user will send the signed item.

1 27. The apparatus of claim 25, wherein the authorization mechanism is
2 configured to determine whether the user is authorized to sign the item by
3 communicating with an authority server that is separate from the signature server.

1 28. The apparatus of claim 23, further comprising an authentication
2 mechanism that is configured to allow the user to authenticate the signature server
3 prior to sending the request to the signature server.

1 29. The apparatus of claim 23, further comprising an encryption
2 mechanism that is configured to facilitate encryption of communications between
3 the user and the signature server.

1 30. The apparatus of claim 23, further comprising an initialization
2 mechanism that is configured to:
3 receive a request from an authorized entity to add a new user;
4 generate a key pair for the new user, including a new user private key and
5 a new user public key;
6 communicate with a certification authority to obtain a certificate for the
7 new user based on the key pair; and to
8 store the certificate and the key pair for the new user in a location that is
9 accessible by the signature server to enable the signature server to sign items on
10 behalf of the new user.

1 31. The apparatus of claim 23, further comprising a deletion
2 mechanism that is configured to:
3 receive a request from an authorized entity to delete an old user;
4 notify a certification authority to revoke a certificate for the old user; and
5 to
6 remove the private key for the old user from the signature server, so that
7 the signature server can no longer sign items on behalf of the old user.

1 32. The apparatus of claim 23, further comprising an archiving
2 mechanism that is configured to archive the request and the signed item at the
3 signature server.

1 33. The apparatus of claim 23, further comprising an archiving
2 mechanism that is configured to forward the signed item to an archive server in
3 order to be archived.